## TRAITE COOPERATION EN MATIERE

### **PCT**

REC'D 07 JUN 2004

### RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

PCT

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire	POUR SUITE A DONNER voir la	notification de transmission du rapport d'examen ninaire international (formulaire PCT/IPEA/416)						
mandatano	<u> </u>							
Demande Internationale No. PCT/IB 03/02425	Date du dépôt international (jour/mois/an 10.06.2003	née) Date de priorité (jour/mois/année) 12.06.2002						
Classification internationale des brevets (CIE	3) ou à la fois classification nationale et Cli	3						
H04L9/08	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,							
Dánasant								
Déposant NAGRACARD SA et al.								
1 La présent rapport d'examen préli	iminaire international, établi par l'admi osant conformément à l'article 36.	inistaration chargée de l'examen préliminaire						
2. Ce RAPPORT comprend 5 feuille	es, y compris la présente feuille de co	uverture.						
Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).								
Ces annexes comprennent feuil	les.							
3. Le présent rapport contient des in	ndications et les pages correspondant	es relatives aux points suivants :						
I ⊠ Base de l'opinion								
II ☐ Priorité								
III Absence de formulati	and the state of the							
IV Absence d'unité de l'i	invention							
V 🗵 Déclaration motivée selon la règle 66.2(a)(ii) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration								
d'application industrie	ile, citations et explications à l'appai \	de cette déclaration						
d'application industrie		de cette déclaration						
d'application industrie  VI   Certains documents of		de cette déclaration						
d'application industrie  VI	cités	de cette déclaration						
d'application industrie  VI	cités demande internationale	de cette déclaration						
d'application industrie  VI	cités demande internationale es à la demande internationale	de cette déclaration  rement du présent rapport						
d'application industrie  VI	cités demande internationale es à la demande internationale	de cette deciaration						
d'application industrie  VI	cités demande internationale es à la demande internationale	rement du présent rapport						
d'application industrie  VI	cités demande internationale es à la demande internationale men préliminaire  Date d'achèv  07.06.200	rement du présent rapport						
d'application industrie  VI	cités demande internationale es à la demande internationale men préliminaire  Date d'achèv  07.06.200  chargée de l'examen  s - P.B. 5818 Patentlaan 2 Bas  Holper, G	rement du présent rapport						

# RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale nº

PCT/IB 03/02425

i.	Base	du	rappo	rt
----	------	----	-------	----

		CP				
	le	En ce qui concerne les <b>éléments</b> de la demande internationale (les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans e présent rapport , comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)) :				
	D	escription, Pages				
	1-	telles qu'initialement déposées				
	R	evendications, No.				
	1-	16 telles qu'initialement déposées				
	De	essins, Feuilles				
	1/2	2-2/2 telles qu'initialement déposées				
2		n ce qui concerne la <b>langue</b> , tous les éléments indiqués ci-dessus étaient à la disposition de l'administration lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication ntraire donnée sous ce point.				
	Се	es éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: ,qui est:				
		la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).				
		la langue de publication de la demande internationale (selon la règle 48.3(b)).				
		la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).				
3.		ce qui concerne les <b>séquences de nucléotides ou d'acide aminés</b> divulguées dans la demande ernationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des quences :				
		contenu dans la demande internationale, sous forme écrite.				
		déposé avec la demande internationale, sous forme déchiffrable par ordinateur.				
		remis ultérieurement à l'administration, sous forme écrite.				
		remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.				
		La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.				
		La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie.				
4.	Les	modifications ont entraîné l'annulation :				
		de la description, pages :				

 $\square$  des revendications, nos:

feuilles:

des dessins,

4.

#### RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale nº

PCT/IB 03/02425

comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :	5. 🗆		pport a été formulé abstr au-delà de l'exposé de l'	action faite (de certaine l'invention tel qu'il a été d	s) des modifications, qu déposé, comme il est in	i ont été considérées diqué ci-après (règle
---	------	--	--	--	---	--

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)

- 6. Observations complémentaires, le cas échéant :
- V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- 1. Déclaration

Nouveauté Oui: Revendications 1-16

Non: Revendications

Oui: Revendications 1-16

Possibilité d'application industrielle Non: Revendications Oui: Revendications 1-16

Non: Revendications

2. Citations et explications

Activité inventive

voir feuille séparée

## RAPPORT D'EXAMEN Demande internationale n° PCT/IB03/02425 PRELIMINAIRE INTERNATIONAL - FEUILLE SEPAREE

#### Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

Il est fait référence au document suivant:

D1: WO 97/38530 (DIGCO)

La présente demande concerne un procédé d'échange sécurisé d'informations localement connectés entre eux ainsi qu'un récepteur pour la mise en oeuvre du dit procédé.

L'état de la technique le plus proche est illustré par D1 qui divulgue un procédé d'échange sécurisé d'informations entre un récepteur et un module de sécurité, les deux dispositifs étant localement connectés. Le récepteur comporte une clé publique tandis que le module de sécurité comporte une clé privée correspondante. Le procédé sert à échanger une clé de session aléatoire chiffrée par la clé publique.

Problème dans l'état de la technique: la clé de session peut être imposée par un intrus qui utiliserait ainsi une lacune de sécurité du procédé.

Selon la revendication 1 ce problème est résolu par les étapes consistant à générer un nombre aléatoire différent dans chaque dispositif, chiffrer ce nombre par la première respectivement la seconde clé de la paire de clés, transmettre le nombre chiffré à l'autre dispositif, déchiffrer les nombres chiffrés dans chaque dispositif et combiner les dispositif et combiner les dispositifs pour générer une clé de session utilisée pour l'échange de données entre les deux dispositifs.

Un procédé basé sur le chiffrage de deux nombres aléatoires chiffrés par deux clés différentes de la même paire de clés n'est pas connu ni suggéré par l'état de la technique.

La revendication 1 remplit donc les critères de nouveauté et d'activité inventive de l'article 33(2) et (3) PCT.

Le récepteur selon la revendication 15 est arrangé pour la mise en oeuvre du procédé selon la revendication 1 et remplit donc aussi les critères de nouveauté et d'activité

**BEST AVAILABLE COPY** 

# RAPPORT D'EXAMEN Demande internationale n° PCT/IB03/02425 PRELIMINAIRE INTERNATIONAL - FEUILLE SEPAREE

inventive.

Les caractéristiques supplémentaires des revendications dépendantes 2-14 et 16 définissent des détails de réalisation de sorte que ces revendications sont aussi nouvelles et inventives.

Les procédés et récepteurs revendiqués présentent la possibilité d'activité industrielle.

BEST AVAILABLE COPY